REMARKS

The Office Action dated December 14, 2005, has been received and carefully noted. The following remarks are submitted as a full and complete response thereto. No new matter has been added, and no new issues are raised that require further consideration and/or search. Claims 1-24, 26-54, 56, and 59 are respectfully submitted for consideration.

Initial Matters

Withdrawal of the finality of the Office Action is respectfully requested. As Applicant noted in the Response filed September 23, 2005, the Office Action of June 28, 2005, did not contain answers to Applicants arguments, regardless of whether the amendments were considered. Accordingly, the present response is the first occasion that Applicant has had to rebut the Office Action's response to those arguments.

As explained in MPEP 707.07(f): "Where the applicant traverses any rejection, the examiner should, if he or she repeats the rejection, take note of the applicant's argument and answer the substance of it." Because the Office Action of June 28, 2005, substantially repeated the previous rejection, and because the Office Action of June 28, 2005, did not respond to Applicant's arguments, it is respectfully submitted that this Office Action of December 14, 2005, ought to have been designated as "non-final."

Additionally, the Office Action asserts, at page 14, item 6, that "Applicant's amendment necessitated the new ground(s) of rejection presented in this Office Action."

Applicant respectfully traverses this assertion. Applicant's amendments were clarifying only, and did not necessitate any new grounds of rejection.

Accordingly, withdrawal of the finality of the Office Action is respectfully requested.

Rejections under 35 U.S.C. 103

Claims 1-23, 26-54, and 56 were again rejected under 35 U.S.C. 103(a) as obvious over U.S. Patent No. 5,548,649 of Jacobson ("Jacobson") in view of U.S. Patent No. 5,940,591 of Boyle et al. ("Boyle"). The Office Action states that Jacobson teaches all the features of the claims except the distribution and/or routing of security information between the first network and the second network. The Office Action states that Boyle remedies the deficiencies of Jacobson. Applicant respectfully traverses this rejection.

Claim 1, upon which claims 2-24 are dependent, recites a method for secure communication between a first end terminal located in a first secure network and a second end terminal located in a second secure network. The first and second networks are separated by a relatively insecure intermediate network and a relatively secure intermediate network. The method includes selectively routing, over the relatively insecure intermediate network or the relatively secure intermediate network, a predetermined type of communication identified by a trigger from the first end terminal to the second end terminal over the relatively insecure intermediate network by means of at least one network element triggerable to refer to information held in a storage means to

selectively route the communication according to the information held in the storage means. The method also includes encrypting the selectively routed communication by means of an encryption engine before it traverses the intermediate network. The at least one network element and the encryption engine are located substantially within the first secure network.

Claim 26 recites a method for the distribution of security information between a first node in a first secure network and at least one node in a second secure network. The first and the second networks are separated by a relatively insecure network. Communications from the first node to the at least one second node via the relatively insecure network are encrypted. The method includes the step of providing at least one network element operable to store security information and triggerable to distribute the security information in a secure manner from the first node to at least one target node in the second secure network.

Claim 27, upon which claims 28-36 are dependent, recites a secure network arrangement for communication between a first end terminal located in a first secure network and a second end terminal located in a second secure network. The first and second networks are separated by a relatively insecure intermediate network and a relatively secure intermediate network. The secure network arrangement includes at least one network element triggerable to refer to information held in a storage means to selectively route over the relatively insecure intermediate network or the relatively secure intermediate network a predetermined communication identified by a trigger according to

the information held in the storage means from the first end terminal to the second end terminal. The secure network arrangement also includes an encryption engine for encrypting the selectively routed communication before it traverses the intermediate network. The at least one network element and the encryption engine are located substantially within the first secure network.

Claim 37, upon which claims 38-40 are dependent, recites a secure network arrangement for communication between a first end terminal located in a first secure network and a second end terminal located in a second secure network. The first and second networks are separated by at least one intermediate network. At least one communication route constitutes a relatively insecure communication route and at least one route constitutes a relatively secure communication route from the first end terminal to the second end terminal. The secure network arrangement includes at least one network element triggerable to selectively route a communication from the first end terminal to the second end terminal over the relatively insecure communication route or the relatively secure communication route. The secure network arrangement also includes an encryption engine for encrypting the selectively routed communication before it traverses the relatively insecure intermediate network. The at least one network element and the encryption engine are located substantially within the first secure network.

Claim 41 recites a method for the distribution of security information between a first node in a first secure network and at least one second node in a second secure

network. The first and second networks are separated by a relatively insecure network. Communications from the first node to the at least one second node via the relatively insecure network are encrypted. The method includes providing at least one network element operable to store security information and triggerable to distribute the security information in a secure manner from the first node to at least one target node in the second secure network.

Claims 42, upon which claims 43-54 are dependent, recites a network arrangement for the distribution of security information between a first node in a first secure network and at least one second node in a second secure network. The first and second networks are separated by a relatively insecure network. Communications from the first node to the at least one second node via the relatively insecure network are encrypted. The network arrangement includes at least one network element operable to store security information and triggerable to distribute the security information in a secure manner from the first node to at least one target node in the second secure network.

Claim 56 recites a network arrangement for the distribution of security between a node in a first secure network and at least one node in a second secure network. The first and second networks are separated by a relatively insecure intermediate network. The network arrangement includes, in at least one of the first and second secure networks, at least one network element operable to store security information and triggerable to distribute the security information to at least one target node in the second secure

network. The network arrangement also includes an encryption engine for encrypting a communication before it traverses the relatively insecure intermediate network.

As discussed in the specification, certain embodiments of the present invention enable subscribers to benefit from a secure network service customized according to their own preferences. First and second secure networks are separated by a relatively secure intermediate network and a relatively insecure intermediate network, and a communication is selectively routed over one of these networks. Predetermined types of communication may be selectively routed over the relatively secure intermediate network or the relatively insecure intermediate network depending on information held in the storage means. Additionally, certain embodiments of the present invention enable a network element and the encryption engine to be located substantially in the first network. Thus, encryption circuitry requirements may be reduced. It is respectfully submitted that Jacobson and Boyle, when viewed either singly or in combination, fail to disclose or suggest all the features of any of the presently pending claims. Therefore, the cited references fail to provide the critical and unobvious advantages discussed above.

Jacobson relates to a network local security bridge for bridging first and second sides of a network. Referring to Figure 1 of Jacobson, one network, Ethernet network 100, is shown having secure zones 108-1 to 108-3. A bridge 104-1 is provided for linking side 1 and side 2 of the network. Depending on the destination or source address of the packets received at bridge 104-1, the packets are filtered, and are encrypted before forwarding. Bridge 104-1 includes a number of filter tables, such as Ethernet address

filter table 224-1, that are used to filter packets received dependent on the Ethernet destination address of a packet. For example, Jacobson describes first side packets only being encrypted by the local security bridge if their destination address is within the remote secure zone, but not being encrypted if their destination address is within a remote insecure zone. Second side packets are decrypted if they originate from the remote secure zone, but not if they originate from an insecure zone. After any necessary encryption or decryption, first and second side packets are transmitted to their destination by the local security bridge.

Boyle relates to an apparatus and method for providing network security. Boyle describes a secure network interface unit (SNIU) that controls communications between a respective host or user computer unit, and a network at a session layer of interconnection. Referring to Figure 2, Boyle shows a type "a" network using labels, a type "b" network using labels, and a public network. The networks are separated by a bridge, gateway and guard, each of which forms a SNIU. A bridge SNIU is used between two private networks using the same security labeling semantics but operate at two different protection levels. The gateway SNIU is used between two networks using different security labeling semantics. A guard SNIU is used to support communication between a private network and a public network. According to Boyle, one network may use the labeling terms "top secret," "secret," "confidential," and "unclassified," while a second network uses "most secret," "secret," "restricted," "confidential," and "releasable."

Applicant submits that the combination of cited references does not disclose or suggest all the features of the pending claims. For example, Applicant submits that neither Jacobson nor Boyle discloses or suggests secure networks separated by a relatively insecure network and a relatively secure network. Jacobson describes only one network, or Ethernet network 100. Claim 1 of the present application, for example, includes four networks. Further, Jacobson describes only one route being provided between one end zone and any other end zone, whether the zone is secure or insecure. Boyle also fails to disclose or suggest this feature. Thus, Jacobson and Boyle do not disclose or suggest first and second secure networks separated by a relatively secure intermediate network and a relatively insecure intermediate network.

The Office Action states that Jacobson teaches these features at column 1, lines 47-64 and column 3, line 66 to column 4, line 7. Applicant respectfully disagrees. Neither of those passages discusses a plurality of networks. Indeed, reading those passages in context and with reference to Figure 1, it is apparent that only one network is disclosed.

Specifically, as can be seen at column 1, lines 44-47 and column 4, lines 11-13, the bridge between the two sections of Jacobson's network is a "local network security bridge." Thus the bridge bridges "sides 1 and 2" of the network 100.

Moreover, further evidence can be seen at column 1, lines 8-43. As explained in the "Background of the Invention" portion, Jacobson recognizes a problem for communication between hosts in **a network**. Jacobson asserts that networks connecting

zones or segments of **a network** have been known, but that they have not been able to handle a mixture of encrypted and unencrypted traffic. Accordingly, Jacobson proposes a local network security bridge that bridges "a first side of **a network** and a second side of **the network**." (Emphasis added.) The Office Action's position that Jacobson is applicable to multiple networks is thus fundamentally flawed, because everything having to do with Jacobson's system relates to a segmented local network.

The Office Action responds by noting that Jacobson states, at column 1, lines 10-12, "In these types of networks, each host device is burdened with encrypting outgoing data and decrypting incoming data." Applicant respectfully submits that this comment, taken in context, supports Applicant's position. Specifically, the previous sentence states "Data encryption and decryption for secure communication between hosts in **a network** has existed for many years." (Emphasis added.) Thus, the reference to "such networks" is a reference to networks that each includes data encryption and decryption for secure communication between hosts. In other words, "such networks" is genre language for the class of networks, each of which Jacobson aims to improve.

The Office Action also responds by noting that Boyle provides, at column 4, lines 51-55 of Boyle, two private networks. Applicant respectfully submits that this disclosure is not germane to the rejection, which took the position that Jacobson taught those features. Moreover, it would not have been obvious to one of ordinary skill in the art to modify Jacobson's "local network security bridge" to perform security between networks (internetworking security) as opposed to security within a network (intranetworking

security). There is especially is no such motivation to modify Jacobson on the limited basis that Boyle happens to disclose a plurality of networks. Accordingly, it is respectfully submitted that the Office Action's position that Jacobson teaches that its "local network security bridge" is between two networks is fundamentally flawed, and that one of ordinary skill in the art would not have been motivated to undo the whole purpose of Jacobson to provide security within **a network** by changing the "local network security bridge" into some other kind of bridge, as the Office Action appears to suggest.

Moreover, claim 1 currently recites four networks: a first secure network, a second secure network, a relatively insecure intermediate network, and a relatively secure intermediate network.

The Office Action specifically referred to Jacobson's figure 1. Figure 1 of Jacobson discloses an Ethernet network 100 comprising secure zones 108-1 to 108-3. A bridge 104-1 is provided for linking two sides, side 1 and side 2, of the network. Depending on the destination or source address of packets received at bridge 104-1, the packets may be filtered, and may be encrypted before forwarding. Bridge 104-1 includes a number of filter tables, for example Ethernet address filter table 224-1 which is used to filter packets received dependent on the Ethernet destination address of a packet.

Even if secure zone 108-1, 108-2, and 108-3 were interpreted as being "secure networks," (not admitted) Jacobson fails to disclose secure networks separated by a relatively secure and a relatively insecure network. As can be shown in the enclosed

marked-up version of Jacobson's Figure 1, the only network that links the host units in the secure zones is the "insecure" Ethernet network 100. Furthermore, only one route is ever provided between one end zone in Jacobson and any other end zone.

In contrast, claim 1 recites first and second secure networks separated by a relatively secure intermediate network and a relatively insecure intermediate network, and a communication is selectively routed over one of these networks.

Applicant also submits that the cited references fail to disclose or suggest selectively routing, over the relatively insecure intermediate network or the relatively secure intermediate network, a predetermined type of communication. Further, applicant submits that the cited references do not disclose or suggest selectively routing a packet over one of a relatively secure intermediate network and a relatively insecure intermediate network by a network element triggerable to refer to information held in a storage means. For example, as discussed above, Jacobson describes using one network with a bridge linking two sides of the network. A packet is filtered, and in some cases encrypted, according to filter tables and depending on the destination address of the packet.

Applicant also submits that the cited references do not disclose or suggest storage means to selectively route the communication. Instead, for example, Jacobson describes using the destination address and the filter table to route a packet. Applicant submits Boyle also does not disclose or suggest these features. Thus, applicant submits that the cited references do not disclose or suggest at least these features of the pending claims.

The previous Office Action mailed June 28, 2005, had not explicitly indicated how Jacobson teaches these features, and since some of these features are predicated on the presence of a plurality of networks, as opposed to Jacobson's single network, it is unclear how they could be construed to be taught by Jacobson.

The present Office Action responded that the features were shown in Figures 2 and 4a-4c of Jacobson. Applicant respectfully disagrees. Figure 2 is a block diagram of a network security bridge, and Figures 4a-4c are the detailed flow of operation of the same network security bridge. As explained at column 4, lines 11-13, this "network local security" bridge bridges "sides 1 and 2" of the network. Accordingly, the network local security bridge 104-1 cannot perform "selectively routing, over the relatively insecure intermediate network or the relatively secure intermediate network, a predetermined type of communication."

The Office Action states that Jacobson does not "explicitly point out the distribution and/or routing of security information between the first network and the second network." Applicant submits that Boyle, either alone or in combination with Jacobson, also does not disclose or suggest the feature of routing security information. As discussed above, Boyle describes data classified as "secret" or "most secret" being distributed between networks. Boyle, however, does not disclose or suggest the distribution of security information between networks. Applicant submits that the data with a high security rating or clearance of Boyle does not disclose or suggest security information that defines security parameters. For example, security information, as

claimed, may include encryption/decryption information and electronic cash bit strings. Applicant submits that Boyle fails to disclose or suggest the distribution or selectively routing of security information. Thus, Jacobson and Boyle fail to disclose or suggest at least these features of the pending claims.

Applicant notes that the arguments relating to security information as opposed to confidentiality classifications (such as secret, most secret, etc.) remain unanswered and unaddressed **yet again** by the Office Action. Applicant notes that the ordinary meaning of "security" in the realm of network security does not include confidentiality classifications used to classify secrets. There is nothing in the present specification that would lead one to conclude that the ordinary meaning of the term "security" has been altered by the Applicant, and therefore the accidental use of the term "security" with a different meaning in Boyle is not a proper basis for rejecting the claims.

Thus, Applicant submits that the cited references do not disclose or suggest "selectively routing, over one of said relatively insecure intermediate network and said relatively secure intermediate network, a predetermined type of communication identified by a trigger from the first end terminal to the second end terminal over said relatively insecure intermediate network by means of at least one network element triggerable to refer to information held in a storage means," as recited in claim 1. Claim 27 recites "at least one network element triggerable to refer to information held in a storage means to selectively route over one of said relatively insecure intermediate network and said relatively secure intermediate network." Applicant submits that the cited references,

either alone or in combination, does not disclose or suggest at least these features of the pending claims. The remaining independent claims recite subject matter similar to claim 1 and/or claim 27 and are allowable for at least the reasons given above. Thus, for at least the reasons given above, the remaining independent claims 26, 27, 37, 41, 42 and 56 are not disclosed or suggested by the cited references.

Claims 2-23 and 28-36 and 38-40 and 43-54 are directly or indirectly dependent upon the independent claims discussed above. The dependent claims are allowable at least for the reasons given above, and because they recite subject matter in addition to the subject matter of the independent claims. Thus, it is submitted that claims 1-23, 26-54 and 56 are not disclosed or suggest by the cited references, either alone or in combination. Applicant respectfully requests that the obviousness rejection of these claims be withdrawn.

Claims 24 and 59 were again rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Jacobson in view of U.S. Patent No. 6,421,339 (Thomas). The Office Action took the position that Jacobson does not teach providing the routing and/or access point to a subscriber in a visited network by virtue of a roaming agreement between the operator of the visited network and the operator of the subscriber's home network. The Office Action then took the position that Thomas taught those features of the claims missing from Jacobson. Applicant respectfully traverses the obviousness rejection and submits that the cited references, either alone or in combination, do not disclose or suggest all the features of the presently pending claims.

Claim 24 depends directly from claim 1. Claim 1 is summarized above. Applicant submits that claim 24 recites the features of claim 1, and also recites the features of the selectively routing step including providing the routing to a subscriber in a visited network by virtue of a roaming agreement between an operator of the visited network and an operator of the subscriber's home network.

Claim 59 depends indirectly from claim 1. Applicant submits that claim 59 recites the features of claim 1, and also recites the features of the providing step including providing the access point to a subscriber in a visited network by virtue of a roaming agreement between an operator of the visited network and an operator of the subscriber's home network.

Thomas relates to methods and systems for call-forwarding. Thomas describes a compliant data packet network with a registering function whereby home-based users are identified separate from visiting users having other networks as home bases. The user location data of Thomas may be retrieved and modified as those users roam to other compliant networks and register with a gatekeeper at that visited network. The registration of a visiting user with a visited gatekeeper includes the process of assigning a transient identity to the roaming user, obtaining confirmation from the home gatekeeper that roaming is authorized when registering the roaming user's present address and transient identity at the home site so that calls received at the home network can be directed to the user at the visited site.

Applicant submits that Jacobson and Thomas, either alone or in combination, do not disclose or suggest selectively routing, over one of the relatively insecure intermediate network and the relatively secure intermediate network, a predetermined type of communication identified by a trigger from the first end terminal to the second end terminal over the relatively insecure intermediate network by means of at least one network element triggerable to refer to information held in a storage means. Thomas describes home-based users being identified separate from visiting users having other networks as home bases. Thomas does not disclose or suggest selectively routing a predetermined type of communication over a relatively insecure intermediate network by means of one or more network elements according to information in a storage means. Therefore, applicant submits that Thomas, either alone or in combination with Jacobson, does not disclose or suggest all the features of the pending claims.

Further, claims 24 and 59 are directly or indirectly dependent upon independent claim 1. If an independent claim is nonobvious, then any claim depending therefrom also is nonobvious. MPEP 2143.03. Because independent claim 1 is nonobvious over the cited references, claims 24 and 59 also are nonobvious. Thus, claims 24 and 59 are not rendered obvious by the cited references and applicant respectfully requests that the obviousness rejection be withdrawn.

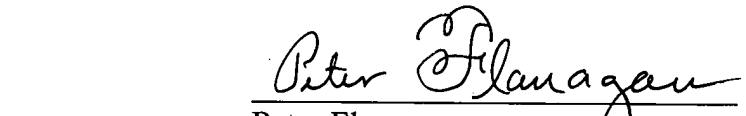
Conclusion

Accordingly, for the reasons explained above it is respectfully submitted that each of claims 1-24, 26-54, 56, and 59 recites subject matter that is neither disclosed nor suggested in the cited art. It is therefore respectfully requested that claims 1-24, 26-54, 56, and 59 be allowed, and that this application be passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicant's undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



Peter Flanagan
Registration No. 58,178

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802
PCF:kmp

Enclosure: Marked-Up Copy of Jacobson's Figure 1

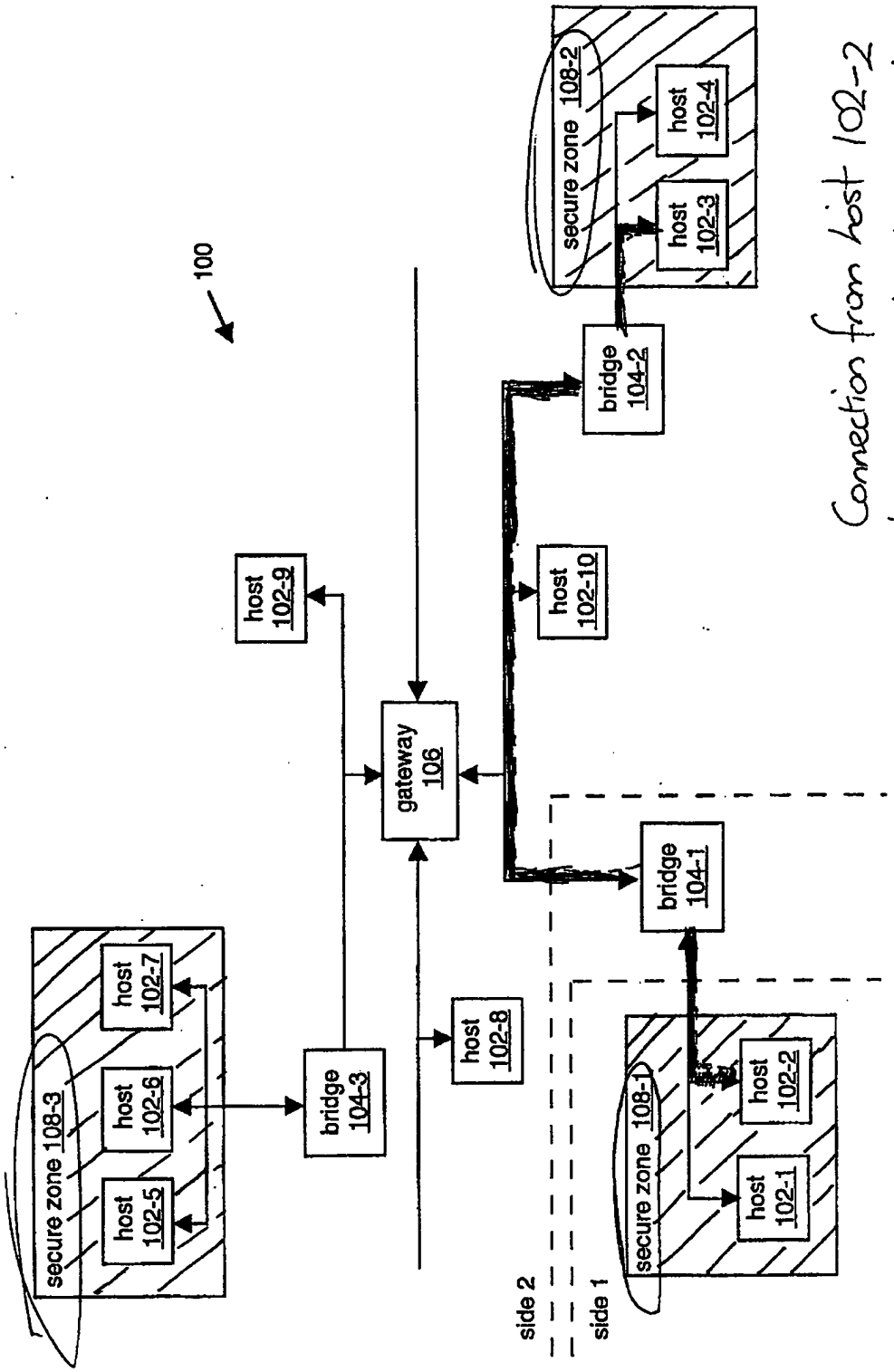


Figure 1

Connection from host 102-2 to 102-3 - travels only via relatively insecure network ie between bridge 104-1 & bridge 104-2.